伽罗瓦域 $GF(2^8)$上高矩阵为密钥的 Hill 加密衍生 *

刘海峰 [a, b]，卢开毅 [a]，梁星亮 [b]

(陕西科技大学 a. 电气与信息工程学院; b. 文理学院, 西安 710021)

摘　要：针对传统的 Hill 加密算法仅是利用伽罗瓦域 GF(p)上可逆的数字方阵作为密钥矩阵与明文向量做模 p 乘法进行加密运算，提出了一种新的在伽罗瓦域 GF(2)[x]/p(x)上以多项式高矩阵作为密钥矩阵的 Hill 加密衍生算法。在 Hill 加密衍生算法中，明文向量为明文字符对应的多项式构成的多项式向量，随机选取密钥矩阵的一列作为加密时的平移增量，在 GF(2)[x]/p(x)上进行密钥矩阵与明文向量的模 8 次不可约多项式 p(x)的乘法和加法，然后获得元素为多项式的密文向量，从而实现明文信息加密。当攻击者在不知道 p(x)、密钥矩阵以及随机抽取的平移向量的情况下由密文破解得到明文的难度更大，从而提高了伽罗瓦域 GF(2)[x]/p(x)上 Hill 加密衍生算法的抗攻击能力。

关键词：伽罗瓦域 GF(2)[x]/p(x)；Hill 加密；多项式高矩阵；不可约多项式

中图分类号：TN918.4　　doi: 10.3969/j.issn.1001-3695.2018.03.0228

Hill encryption derivative algorithm in galois field $GF(2^8)$ with high-matrix as key matrix

Liu Haifeng[a, b], Lu Kaiyi[a], Liang Xingliang[b]

(*a. College of Electrical & Information Engineering, b. College of Arts & Sciences, Shannxi University of Science & Technology, Xi'an* 710021, *China*)

Abstract: In traditional Hill encryption algorithm, the modulo p multiplication of the invertible matrix and plaintext vector in Galois field GF(P) is used to calculate ciphertext vector, this paper proposed a new Hill encryption derivative algorithm in galois field GF(2) [x]/p(x) , which took polynomial high-matrix as key matrix. In this new Hill encryption derivative algorithm, it composed plaintext vector of polynomial derived from corresponding plaintext, it selected a column of key matrix as translation increment randomly modulo eighth degree irreducible polynomial p(x) multiplication of the polynomial high-matrix and plaintext vector in Galois field GF(2) [x]/p(x) was done, then modulo eighth degree irreducible polynomial p(x) addition of the product and translation increment in Galois field GF(2) [x]/p(x) was carried out, thus it obtained the polynomial ciphertext vector, and achieved the purpose of encrypting the plaintext messages. Because it is more difficult to get plaintext from ciphertext under the condition that p(x) , key matrix and random selected translation vector are unknown, the new Hill encryption derivative algorithm in Galois field GF(2) [x]/p(x) improve the capability for anti-attack.

Key words: Galois field GF(2)[x]/p(x); Hill encryption; polynomial high-matrix; irreducible polynomial

0　引言

伽罗瓦域亦称有限域[1,2]，其域的元素是有限的。传统的 Hill 加密算法将英文字母、数字以及常见的符号构成编码字符集，编码字符集的基数为 p，以一定的规则进行编码，并对应到 0～ $p-1$之间的整数。但是如果编码字符集的基数 p 不为素数[3]，还需要注意到必须要使得加密矩阵行列式的值在模 p 下有乘法逆元。文献[4,5]给出了在模 26 情况下的数字方阵作为密钥矩阵所需要满足的要求，并给出了在模 26 意义下选取密钥矩阵的方法。文献[6]针对密钥矩阵在模 26 意义下的逆矩阵可能是分数的问题提出了行列变换的改进；当 p 为素数时，可以得到一个具有 p 个元素的伽罗瓦域 $GF(p)$，但其上的 Hill 加密的密钥矩阵仍然十分脆弱。

伽罗瓦域 $GF(2^8)$ 是一种特殊的有限域[7]，其具有 2^8 个元素，而不是像有限域 $GF(p)$ 上必须有 p 个元素(p 为素数)。有限域 $GF(2^8)$ 上每个元素都可以表示为 8 位的二进制数，并可以将元素唯一地映射为一个系数为 0、1 的 8 次以下的一元多项式，其有限域上多项式的加法和乘法等运算具有封闭性，在密码学、信息编码等领域都是很重要的数学工具[8]，有限域 $GF(2^8)$ 的算术运算还具有一定复杂性和特殊性，相比于传统的

收稿日期：2018-03-29；**修回日期：**2018-05-16　　**基金项目：**陕西省自然科学基础研究计划—青年项目（2017JQ1026）；陕西省教育厅专项科学研究计划项目（17JK0102）

作者简介：刘海峰（1964-），男，陕西泾阳人，副教授，硕士，主要研究方向为计算机网络与信息安全、代数编码与密码学（1977645503@qq.com）；卢开毅（1992-），男，重庆人，硕士研究生，主要研究方向为密码学、网络信息安全；梁星亮（1987-），男，甘肃定西人，讲师，主要研究方向为半群代数理论.

Hill 加密而言在很大程度上提高了算法的安全性。

本文论述有限域 $GF(2^8)$ 上的 Hill 加密是对传统 Hill 加密的衍生，把有限域 $GF(2^8)$ 上互为伪逆的一对矩阵作为加密和解密密钥，能满足安全密码系统的基本条件。本文选取空格和 255 个互异的可见字符进行字符编码，如表 1 所示，并按照 $0\sim255$ 的顺序对表格中的字符按照行优先进行编码。

表 1　字符编码

space	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
r	s	t	u	v	w	x	y	z	A	B	C	D	E	F	G	H	I
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	0
1	2	3	4	5	6	7	8	9	!	@	#	$	%	^	&	*	(
)	-	_	=	+	~	`	[	]	\	;	,	.	/	{	}	:	"
'	<	>	?	α	β	γ	δ	ε	ζ	η	θ	ι	κ	λ	μ	ν	ξ
ο	π	ρ	σ	τ	υ	φ	χ	ψ	ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ
Ι	Κ	Λ	Μ	Ν	Ξ	Ο	Π	Ρ	Σ	Τ	Υ	Φ	Χ	Ψ	Ω	℃	℉
Ⅰ	Ⅱ	Ⅲ	Ⅳ	Ⅴ	Ⅵ	Ⅶ	Ⅷ	Ⅸ	Ⅹ	Ⅺ	Ⅻ	ⅰ	ⅱ	ⅲ	ⅳ	ⅴ	ⅵ
ⅶ	ⅷ	ⅸ	ⅹ	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М
Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю
Я	★	☆	▲	△	◆	◇	■	□	⊙	○	▽	『	』	〖	〗	《	》
〔	〕	「	」	【	】	£	¢	￥	←	↑	→	↓	↖	↗	↘	↙	∈
√	∞	∽	≈	∵	∷	※	≌	∫	≦	≧	≮	≯	≡	≠	×	÷	±
•	≤	≥	§	(表中的 space 表示空格符)													

1　伽罗瓦域 $GF(2)[x]/p(x)$ 的定义

$GF(2)[x]$ 的定义：$GF(2)[x]$ 指二元域 $GF(2)$ 上的一元多项式全体的集合。

设 $p(x)$ 是 $GF(2)$ 上的一个 8 次不可约多项式，$GF(2)[x]/p(x)=<S,+,*,p(x)>$ 是一个代数结构，有 $S=\{a(x)\,|\,a(x)\in GF(2)[x],\deg(a(x))<8\}$，且 $GF(2)[x]/p(x)$ 关于有限域上的加法构成阿贝尔群，其单位元为零多项式，$GF(2)[x]/p(x)-\{0\}$ 关于有限域上的乘法"*"构成阿贝尔群，且"*"对"+"满足左右分配律，也即对 $\forall a(x),b(x),c(x)\in S$，本文记 $a(x)=\sum_{i=0}^{7}a_ix^i$，$b(x)=\sum_{i=0}^{7}b_ix^i$，$c(x)=\sum_{i=0}^{7}c_ix^i$，其中系数有 $a_i,b_i,c_i\in\{0,1\}$，满足左右分配律 $(a(x)+b(x))*c(x)=a(x)*c(x)+b(x)*c(x)$，$c(x)*(a(x)+b(x))=c(x)*a(x)+c(x)*b(x)$ 成立。考虑到 $GF(2^8)$ 与 $GF(2)[x]/p(x)$ 上的元素及其元素间相应的运算具有一一对应的同构的性质，因此从结构上讲，同构的对象是完全等价的，所以下文重点讨论 $GF(2)[x]/p(x)$ 上的 Hill 加密衍生算法。伽罗瓦域 $GF(2)[x]/p(x)$ 上相应的运算定义如下：

$$a(x)+b(x)=\sum_{i=0}^{7}((a_i+b_i)\bmod 2)x^i$$

$a(x)-b(x)=a(x)+b(x)$

$a(x)*b(x)=(\sum_{i=0}^{7}\sum_{j=0}^{7}((a_i\times b_j)\bmod 2)x^{i+j})\bmod p(x)$

$a(x)^{-1}$：当且仅当 $a(x)*a(x)^{-1}=1$

$a(x)/b(x)=a(x)*b(x)^{-1}$

2　伽罗瓦域 $GF(2)[x]/p(x)$ 上多项式和多项式矩阵的求逆

2.1　伽罗瓦域 $GF(2)[x]/p(x)$ 的多项式求逆

对 $\forall a(x)\in GF(2)[x]/p(x),a(x)\neq0$，因为 $p(x)$ 为不可约多项式，显然有 $\gcd(a(x),p(x))=1$，根据代数性质，必然存在有限域上的唯一的多项式 $b(x)$ 使得 $b(x)=a(x)^{-1}$ 为 $a(x)$ 的乘法逆元。可用如下方法求多项式 $a(x)$ 的逆多项式：

a)　令 $a(x)=a_kx^k+\cdots+a_2x^2+a_1x+a_0$，其中有 $a_i\in\{0,1\}$，$k\le7$。

b)　设 $b(x)$ 是 $a(x)$ 在模 $p(x)$ 下的逆多项式，令 $b(x)=b_7x^7+\cdots+b_2x^2+b_1x+b_0$，其中 $b_i\in\{0,1\}$。

c)　由多项式的乘法可得 $c(x)=a(x)*b(x)=a_kb_7x^{k+7}+(a_{k-1}b_7+a_kb_6)x^{k+6}+\cdots+a_0b_0$ 也即有

$$c(x)=(x^{k+7},x^{k+6},\cdots,x^7,\cdots,x^2,x,1)\begin{pmatrix}a_k&0&0&\cdots&0&\cdots&0&0\\a_{k-1}&a_k&0&\cdots&0&\cdots&0&0\\a_{k-2}&a_{k-1}&a_k&\cdots&0&\cdots&0&0\\\vdots&\vdots&\vdots&&\vdots&&\vdots&\vdots\\a_1&a_2&a_3&\cdots&a_k&\cdots&0&0\\a_0&a_1&a_2&\cdots&a_{k-1}&\cdots&0&0\\0&a_0&a_1&\cdots&a_{k-2}&\cdots&0&0\\\vdots&\vdots&\vdots&&\vdots&&\vdots&\vdots\\0&0&0&\cdots&0&\cdots&a_0&a_1\\0&0&0&\cdots&0&\cdots&0&a_0\end{pmatrix}\begin{pmatrix}b_7\\b_6\\b_5\\b_4\\b_3\\b_2\\b_1\\b_0\end{pmatrix}$$

其中的二维矩阵是一个 $(k+8)\times8$ 的矩阵，可以把 $c(x)$ 中方次大于 7 的项 $x^m(m>7)$ 用模 $p(x)$ 的余式替换掉，也即在伽罗瓦域 $GF(2)[x]/p(x)$ 中用 $x^m\bmod p(x)$ 得到的结果替换掉 x^m，从而消去 x 的方次大于 7 的项，替换后合并同类项得到降幂的多项式 $c(x)=c_7x^7+\cdots+c_2x^2+c_1x+c_0$，其中 c_i 包含未知数 $b_7,b_6,\cdots.b_1,b_0$。

d)　由于设 $b(x)$ 是 $a(x)$ 在模 $p(x)$ 下的逆多项式，所以 $c(x)=a(x)*b(x)=1\bmod p(x)$，也即可以得到

$c(x)=c_7x^7+\cdots+c_2x^2+c_1x+c_0=1 \bmod p(x)$，又因为 $c(x)\in GF(2)[x]/p(x)$，所以可以得到 $c(x)=c_7x^7+\cdots+c_2x^2+c_1x+c_0=1$，因此有下面的方程组成立

$$\begin{cases} c_7(b_7,b_6,\cdots,b_2,b_1,b_0)=0 \\ \vdots \\ c_1(b_7,b_6,\cdots,b_2,b_1,b_0)=0 \\ c_0(b_7,b_6,\cdots,b_2,b_1,b_0)=1 \end{cases}$$

用模 2 下的高斯消元法解此方程组，最后即可得 $b(x)$ 中各项的系数，得到 $a(x)$ 的逆多项式 $b(x)$。

2.2 伽罗瓦域 $GF(2)[x]/p(x)$ 的方阵求逆

设有限域上的 n 阶多项式方阵 $Key(x)$ 满足 $Key(x)=\begin{bmatrix} a_{11}(x) & a_{12}(x) & \cdots & a_{1n}(x) \\ a_{21}(x) & a_{22}(x) & \cdots & a_{2n}(x) \\ \vdots & \vdots & & \vdots \\ a_{n1}(x) & a_{n2}(x) & \cdots & a_{nn}(x) \end{bmatrix}$，其中有 $a_{ij}(x)\in GF(2)[x]/p(x)$，先根据代数学方法求 $Key(x)$ 在有限域 $GF(2)[x]/p(x)$ 上的行列式 $\det(Key(x))=|Key(x)| \bmod p(x)$，$|Key(x)|$ 为矩阵 $Key(x)$ 的普通 n 阶行列式。定义伴随矩阵 $Key(x)^*=\begin{bmatrix} A_{11}(x) & A_{21}(x) & \cdots & A_{n1}(x) \\ A_{12}(x) & A_{22}(x) & \cdots & A_{n2}(x) \\ \vdots & \vdots & & \vdots \\ A_{1n}(x) & A_{2n}(x) & \cdots & A_{nn}(x) \end{bmatrix}$，其伴随矩阵中的 $A_{ij}(x)$ 为多项式方阵 $Key(x)$ 中元素 $a_{ij}(x)$ 在模 $p(x)$ 意义下的对应的代数余子式。如果有 $\det(Key(x))\neq 0$，则可以根据上节的有限域 $GF(2)[x]/p(x)$ 上多项式求逆的方法可以求得多项式 $\det(Key(x))$ 的逆多项式 $|Key(x)|^{-1}$，最后逆矩阵 $Key(x)^{-1}=(|Key(x)|^{-1}\cdot Key(x)^*) \bmod p(x)$。

2.3 伽罗瓦域 $GF(2)[x]/p(x)$ 的多项式高矩阵左伪逆求解

线性代数中的高矩阵[10]：指诸列线性无关的矩阵叫做高矩阵。可逆方阵为高矩阵的一种特例。

伽罗瓦域 $GF(2)[x]/p(x)$ 上的多项式高矩阵：有限域 $GF(2)[x]/p(x)$ 上的高矩阵指列满秩的多项式矩阵，其中多项式矩阵的元素属于 $GF(2)[x]/p(x)$，$p(x)$ 是 $GF(2)$ 上的一个 8 次不可约多项式。

根据一般的数字高矩阵 A 求左伪逆的公式 $pinv(A)=(A'*A)^{-1}*A'$ [11](其中 A 为列满秩的数字矩阵)，可得伽罗瓦域 $GF(2)[x]/p(x)$ 上高矩阵求左伪逆的方法，可以设加密的密钥高矩阵 $A(x)=\begin{bmatrix} a_{11}(x) & a_{12}(x) & \cdots & a_{1l}(x) \\ a_{21}(x) & a_{22}(x) & \cdots & a_{2l}(x) \\ \vdots & \vdots & & \vdots \\ a_{k1}(x) & a_{k2}(x) & \cdots & a_{kl}(x) \end{bmatrix}$ 是列满秩的矩阵，且高矩阵 $A(x)$ 的行和列满足 $k\geq l$，则有 $(A(x)'*A(x))_{ij}=(\sum_{t=1}^{k}a_{ti}(x)a_{tj}(x)) \bmod p(x)$，其中 $(i,j=1,2\cdots,l)$，然后利用上节伽罗瓦域 $GF(2)[x]/p(x)$ 上多项式方阵求逆的方法可求得 $A'(x)*A(x)$ 在模 $p(x)$ 意义下的逆多项式矩阵 $(A'(x)*A(x))^{-1}$，最后用求得的 $(A'(x)*A(x))^{-1}$ 与 $A'(x)$ 做模 $p(x)$ 的多项式矩阵的乘法，即可求得高矩阵 $A(x)$ 的左伪逆矩阵 $pinv(A(x))$。

3 伽罗瓦域 $GF(2)[x]/p(x)$ 上的 Hill 加密衍生算法及其解密算法

文献[12~14]提出了有限域上有关衍生的 Hill 加密以及分组加密的思想，其中包括利用有限域上圆锥曲线密码体制等结合 Hill 分组加密来保证数据的安全，本文对一般的 Hill 加密算法做了如下衍生。

3.1 伽罗瓦域 $GF(2)[x]/p(x)$ 上的 Hill 加密衍生算法

假设由字符编码集中的字符构成明文字符串 $M=M_1M_2\cdots M_m$，现需要对明文进行加密发送，首先选取伽罗瓦域上合适的列满秩的加密矩阵 $eKey(x)=\begin{bmatrix} a_{11}(x) & a_{12}(x) & \cdots & a_{1l}(x) \\ a_{21}(x) & a_{22}(x) & \cdots & a_{2l}(x) \\ \vdots & \vdots & & \vdots \\ a_{k1}(x) & a_{k2}(x) & \cdots & a_{kl}(x) \end{bmatrix}$（其中有 $k>l$）和一个 8 次不可约多项式 $p(x)$，若明文字符串的长度 m 不满足 $l\,|\,m$，则根据文献[15]处理哑元的方法，添加 i 个空格字符作为哑元构成新的明文字符串 $M=M_1M_2\cdots M_k\cdots M_m\cdots M_{m+i}$，使 $l\,|\,(m+i)$，其中 $i<l$，加密时对字符串 M 按 l 个字符为一组进行分组，然后对每一组进行 Hill 加密，对加密后的字符串不做更改。

不妨设取分组中的第一组字符进行加密，取 M 的前 l 个字符 $M_1M_2\cdots M_l$，对其中的每个字符 $M_j(1\leq j\leq l)$ 在字符编码表 1 中查询其对应位置的索引值 $Index_j$，并将对应位

置的索引值 $Index_j$ 转换成对应的二进制形式的表达式，也即有 $Index_j = m_{j_7} * 2^7 + m_{j_6} * 2^6 + \cdots + m_{j_1} * 2 + m_{j_0}$，把式中的 2 替换为 x 可以得到多项式 $f_j(x) \in GF(2)[x]/p(x)$，最后可以得到一个明文字符串 $M_1 M_2 \cdots M_l$ 所对应的一个多项式向量 $f(x) = [f_1(x) \quad f_2(x) \quad \cdots \quad f_l(x)]^T$，在伽罗瓦域上左乘加密矩阵 $eKey(x)$，并选取密钥矩阵的第 l 列(也可以随机选取密钥矩阵的其他列)作为平移增量，利用加密矩阵进行 Hill 加密后的密文向量 $e(x)$，其中 $e(x) = [e_1(x) \quad e_2(x) \quad \cdots \quad e_k(x)]^T$，向量分量满足有 $e_j(x) = ((\sum_{i=1}^{l} a_{ji}(x) * f_i(x)) + a_{jl}(x)) \bmod p(x)$，$j = 1, 2 \cdots, k$。上式用矩阵的形式来表示即为 $e(x) = (eKey(x) * f(x) + a_{\cdot l}(x)) \bmod p(x)$，其中 $a_{\cdot l}(x)$ 表示抽取矩阵 $eKey(x)$ 中的第 l 列。将密文多项式向量中每个多项式中的变量 x 用 2 替换，并求多项式的值，也即得到加密后密文字符在字符编码表中所对应的索引值，通过查表转换即可得到密文字符串 $C_1 C_2 \cdots C_l \cdots C_k$。

3.2 伽罗瓦域 $GF(2)[x]/p(x)$ 上的 Hill 加密衍生算法的解密

先根据上节的方法求加密矩阵 $eKey(x)$ 在有限域 $GF(2)[x]/p(x)$ 的左伪逆矩阵，并记左伪逆矩阵为 $dKey(x)$，使得求解得到的 $dKey(x)$ 作为解密矩阵。

$$dKey(x) = \begin{bmatrix} b_{11}(x) & b_{12}(x) & \cdots & b_{1k}(x) \\ b_{21}(x) & b_{22}(x) & \cdots & b_{2k}(x) \\ \vdots & \vdots & & \vdots \\ b_{l1}(x) & b_{l2}(x) & \cdots & b_{lk}(x) \end{bmatrix}$$

，其中，由于加密时已经对相应的哑元进行了替换处理，所以 加密后的密文字符串的长度必然为 $k(m+i)/l$，且有 $l \mid (m+i)$，因此可以直接对密文字符串 $C = C_1 C_2 \cdots C_k \cdots C_m \cdots C_{k(m+i)/l}$ 以 k 个字符为一组进行分组，再对每一组进行解密运算。

现在对分组中的其中一组密文字符讨论解密算法，不妨取 C 的第 1 组的 k 个字符 $C_1 C_2 \cdots C_k$，对其中的每个字符 $C_j (1 \le j \le k)$ 在字符编码表中查询其对应位置的索引值 $Index_j$，并将对应的索引值 $Index_j$ 转换成对应的二进制形式的表达式，也即有 $Index_j = c_{j_7} * 2^7 + c_{j_6} * 2^6 + \cdots + c_{j_1} * 2 + c_{j_0}$，同时把表达式中的 2 替换为 x 可以得到多项式 $g_j(x) \in GF(2)[x]/p(x)$，最后可以得到一个密文字符串 $C_1 C_2 \cdots C_k$ 所对应的一个多项式向量 $g(x) = [g_1(x) \quad g_2(x) \quad \cdots \quad g_k(x)]^T$，在有限域上先减去平移增量(即密钥矩阵的第 l 列)，再用得到的结果右乘解密矩阵 $dKey(x)$，然后可以得明文向量 $d(x)$，其中明文向量 $d(x) = [d_1(x) \quad d_2(x) \quad \cdots \quad d_l(x)]^T$，$d_j(x) = (\sum_{i=1}^{k} b_{ji}(x) * (g_i(x) - a_{il}(x))) \bmod p(x)$，$j = 1, 2 \cdots, l$。以上的式子用矩阵形式来表示即为 $d(x) = (dKey(x) * (g(x) - a_{\cdot l}(x))) \bmod p(x)$，其中 $a_{\cdot l}(x)$ 表示抽取矩阵 $eKey(x)$ 中的第 l 列。将明文多项式向量中每个多项式中的变量 x 用 2 替换，并求多项式的值，即得到解密后明文字符在字符编码表中所对应的索引值，通过查表转换即可得到明文字符串 $M_1 M_2 \cdots M_l$。

4 多项式环 $GF(2)[x]$ 中 8 次不可约多项式

$GF(2)[x]$ 上的 8 次不可约多项式是指系数只能为 0、1 的 8 次不可约的一元多项式，即 8 次不可约多项式 $p(x) = x^8 + a_7 x^7 + \cdots + a_1 x + a_0$（其中 $a_7, \cdots, a_1, a_0 \in \{0,1\}$），满足不能分解成 $GF(2)[x]$ 上 7 次及 7 次以下的多项式的乘积。为了求解 $GF(2)[x]$ 上的 8 次不可约多项式的集合 A，可以先通过遍历相乘的方法求出多项式环 $GF(2)[x]$ 上的 8 次可约多项式的集合 B：通过分析，$GF(2)[x]$ 上的 8 次可约多项式的集合可以表示为 $B = B_1 \cup B_2 \cup B_3 \cup B_4$，其中 B_1 为任意 1 次和任意 7 次多项式乘积的集合，B_2 为任意 2 次和任意 6 次多项式乘积的

集合，B_3 为任意 3 次和任意 5 次多项式乘积的集合，B_4 为任意两个 4 次多项式乘积的集合。然后利用 $GF(2)[x]$ 上的 8 次多项式的全集 S 对 B 作差集运算，即可得相应的 8 次不可约多项式的集合 $A=S-B$。其多项式环上 8 次不可约多项式集合求解的 Python 程序如下所示：

```
import numpy
import math
C = []
for i in range(1, 5): #[1 2 3 4]
    j = 8-i
    A = []
    B = []
    for row in range(1, int(math.pow(2, i))+1):# 从1取到2^i
        tempList = []
        for x in list((bin(row))[2:].zfill(i+1)):
            tempList.append(int(x))
        tempList[0] = 1
        A.append(tempList)
    for row in range(1, int(math.pow(2, j))+1):# 从1取到2^j
        tempList = []
        for x in list((bin(row))[2:].zfill(j+1)):
            tempList.append(int(x))
        tempList[0] = 1
        B.append(tempList)
    for i1 in range(int(math.pow(2, i))):
        for j1 in range(int(math.pow(2, j))):
            p1 = numpy.poly1d(A[i1])
            p2 = numpy.poly1d(B[j1])
            tempCoeffs = (p1 * p2).coeffs
            for x in range(len(tempCoeffs)):
                tempCoeffs[x] = tempCoeffs[x] % 2
            C.append(tempCoeffs)

for x in range(len(C)):
    C[x] = list(C[x])
for num in range(256): #0-255
    tempList = [1]
    for x in list((bin(num))[2:].zfill(8)):
        tempList.append(int(x))
    if tempList not in C:
        print(tempList)
```

通过以上 Python 程序的运行结果，即可求得多项式环 $GF(2)[x]$ 上的所有 8 次不可约多项式，其降幂排列时对应的系数向量如表 2 所示。对以上的 Python 程序稍作修改还可以用来求解多项式环 $GF(2)[x]$ 上的 N 次不可约多项式。

表 2　多项式环 GF(2)[x]上所有 8 次不可约多项式的系数向量

[1, 0, 0, 0, 1, 1, 0, 1, 1],	[1, 0, 0, 0, 1, 1, 1, 0, 1],	[1, 0, 0, 1, 0, 1, 0, 1, 1]
[1, 0, 0, 1, 0, 1, 1, 0, 1],	[1, 0, 0, 1, 1, 1, 0, 0, 1],	[1, 0, 0, 1, 1, 1, 1, 1, 1]
[1, 0, 1, 0, 0, 1, 1, 0, 1],	[1, 0, 1, 0, 1, 1, 1, 1, 1],	[1, 0, 1, 1, 0, 0, 0, 1, 1]
[1, 0, 1, 1, 0, 0, 1, 0, 1],	[1, 0, 1, 1, 0, 1, 0, 0, 1],	[1, 0, 1, 1, 1, 0, 0, 0, 1]
[1, 0, 1, 1, 1, 0, 1, 1, 1],	[1, 0, 1, 1, 1, 1, 0, 1, 1],	[1, 1, 0, 0, 0, 0, 1, 1, 1]
[1, 1, 0, 0, 0, 1, 0, 1, 1],	[1, 1, 0, 0, 0, 1, 1, 0, 1],	[1, 1, 0, 0, 1, 1, 1, 1, 1]
[1, 1, 0, 1, 0, 0, 0, 1, 1],	[1, 1, 0, 1, 0, 1, 0, 0, 1],	[1, 1, 0, 1, 1, 0, 0, 0, 1]
[1, 1, 0, 1, 1, 1, 1, 0, 1],	[1, 1, 1, 0, 0, 0, 0, 1, 1],	[1, 1, 1, 0, 0, 1, 1, 1, 1]
[1, 1, 1, 0, 1, 0, 1, 1, 1],	[1, 1, 1, 0, 1, 1, 1, 0, 1],	[1, 1, 1, 1, 0, 0, 1, 1, 1]
[1, 1, 1, 1, 1, 0, 0, 1, 1],	[1, 1, 1, 1, 1, 0, 1, 0, 1],	[1, 1, 1, 1, 1, 1, 0, 0, 1]

5　伽罗瓦域 $GF(2)[x]/p(x)$ 上的 Hill 加密衍生算法和解密的实例验证

假设需要加密传送的字符串为：$string=$ hello, It's nice to meet you。首先选取 $GF(2)[x]$ 上的一个 8 次不可约多项式为 $p(x)=x^8+x^4+x^3+x+1$，并选择伽罗瓦域 $GF(2)[x]/p(x)$ 上的一个 3×2 的列满秩的多项式高矩阵

$$eKey(x)=\begin{bmatrix} x^5 & x^2 \\ x^3 & x^2+1 \\ x^3 & x+1 \end{bmatrix}$$

作为加密时的密钥矩阵，选取密钥矩阵 $eKey(x)$ 的第 2 列 $a._2(x)=\begin{bmatrix} x^2 & x^2+1 & x+1 \end{bmatrix}^T$ 作为加密时候的平移增量，然后可以利用求解高矩阵左伪逆的方法求得解密矩阵 $dKey(x)$：可以先求得对应的行列式 $\det(eKey(x)'*eKey(x))=x^6+x^2+x$，再用多项式求逆的方法得多项式行列式在模 $p(x)$ 下的乘法逆元为 $x^7+x^6+x^5+x^4+x^2+1$，最后根据多项式高矩阵求左伪逆的计算公式可以得 $dKey(x)=$

$$pinv(eKey(x))=(eKey(x)'*eKey(x))^{-1}*eKey(x)'$$

求得密钥矩阵所对应的解密矩阵为

$$dKey(x)=\begin{bmatrix} x^6+1 & x^7+x^3 & x^6+x^5+x^4+x^3+x^2+x+1 \\ x^7+x^6+x^4+x^3 & x^6 & x^3+x^2+1 \end{bmatrix}$$

5.1　加密阶段

第一步　先对以上要加密的字符串中的字符按照表 1 的对应关系转换成相应的数字索引，得到明文字符串索引表如表 3 所示。

表 3　明文字符串索引表

h	e	l	l	o	,	space	I	t	’	s	space	n	i
8	5	12	12	15	83	0	35	20	90	19	0	14	9
c	e	space	t	o	space	m	e	e	t	space	y	o	u
3	5	0	20	15	0	13	5	5	20	0	25	15	21

第二步　由于加密矩阵是 3×2 的高矩阵，所以对明文字符串按照每 2 个字符进行分组，取明文字符串的前两个字符 he 并将其索引转换成 $GF(2)[x]/p(x)$ 上的多项式为 $[x^3,x^2+1]^T$，先左乘加密矩阵，然后加上选取的平移增量 $a._2(x)$ 并在模 $p(x)$ 意义计算可以得到

$$\left(\begin{bmatrix} x^5 & x^2 \\ x^3 & x^2+1 \\ x^3 & x+1 \end{bmatrix}\begin{bmatrix} x^3 \\ x^2+1 \end{bmatrix}+\begin{bmatrix} x^2 \\ x^2+1 \\ x+1 \end{bmatrix}\right) \bmod p(x)=$$

$\begin{bmatrix} x^3+x+1 \\ x^6+x^4+x^2 \\ x^6+x^3+x^2 \end{bmatrix}$，其结果向量多项式的二进制系数构成二进制数，将对应的二进制数转换成十进制数分别为 11、84、76，也即得到了密文字符的索引值，查询字符编码表，可知对应索引的密文字符为 k.+，同理，对其他分组按照相同的方法加密，最后得到加密后的密文字符以及索引如表 4 所示。

表 4　密文字符串索引表

k	.	+	И	"	B	B	Δ	℃	T	Д	ι	Ъ	Ψ
11	84	76	175	89	119	168	121	142	136	170	102	193	140
~	;	ii	Ⅻ	±	:	λ	τ	L	T	.	#	!	§
77	82	157	155	251	88	104	112	12	20	84	65	63	255
Θ	Z	E	H	η	≧	μ	w	γ	Γ	N	E	7	^
125	123	171	24	100	244	105	23	96	120	40	171	60	68

从上面的两表可以看出，通过高矩阵作为密钥加密明文后得到的密文字符的数量是原明文字符数量的 1.5 倍，也即利用高矩阵加密的特点是加密后密文的长度可以不和明文的长度一致。

5.2　解密阶段

第一步　解密阶段应先求出高矩阵的伪逆矩阵。前面已经求出高矩阵 $eKey(x)$ 的左伪逆矩阵 $dKey(x)$。*第二步*　对密文字符串按照 3 个字符为一组进行分组，不妨先取密文字符串的前 3 个字符 k.+并将其对应的索引值转换成有限域上的多项式向量为 $[x^3+x+1, x^6+x^4+x^2, x^6+x^3+x^2]^T$，然后对得到的多项式向量先减去平移增量 $a_2(x)$，再左乘相应高矩阵的左伪逆多项式解密矩阵并在模 $p(x)$ 意义下进行计算，可以得到

$$\begin{bmatrix} x^6+1 & x^7+x^3 & x^6+x^5+x^4+x^3+x^2+x+1 \\ x^7+x^6+x^4+x^3 & x^6 & x^3+x^2+1 \end{bmatrix}\left(\begin{bmatrix} x^3+x+1 \\ x^6+x^4+x^2 \\ x^6+x^3+x^2 \end{bmatrix}-\begin{bmatrix} x^2 \\ x^2+1 \\ x+1 \end{bmatrix}\right) \bmod p(x)=\begin{bmatrix} x^3 \\ x^2+1 \end{bmatrix}$$

其结果向量多项式的二进制系数构成二进制数，将对应的二进制数转换成十进制数分别为 8、5，得到了相应明文字符的索引值，查询字符编码表，可知对应的明文字符为 he，同理，对其他分组按照相同的方法解密，最后即可得到解密的明文字符串 $string=$ hello, It’s nice to meet you。

6　安全性分析

算法安全性取决于密钥的安全性及攻击复杂性，本文所使用的密钥的安全性表现在以下几个方面。

6.1　一次一密通信

本文所使用的密钥矩阵是伽罗瓦域上随机选取的一个多项式高矩阵，本质上它是无法预测的，所以密钥产生的加密函数是安全的，对应的解密函数也是安全的。每次通信时都重新选择密钥矩阵，因而实现了一次一密通信[16]，信息论的创始人 Shannon 已经证明一次一密是绝对安全的，也即之前破解的密钥对之后密文的破解没有任何帮助，一次一密系统在理论上是不可攻破的密码系统[16]。

6.2　雪崩效应

由于 Hill 加密是将明文消息分组混合进行加密，所以明文或者密钥的微小改变都将对密文产生很大的影响，特别是当密钥矩阵的规模更大的时候，明文的某一位发生变化将会导致这一组中的所有密文都发生变化，密钥矩阵的某一位发生变化将会导致每个分组固定位置的密文发生变化，此时这种雪崩效果更加明显，这使得攻击者要直接通过对密文的规律性分析来获得密钥矩阵不可行。

6.3　密钥空间大

$GF(2)[x]/p(x)$ 上的 Hill 加密衍生算法的解密首先要知道正确的 $p(x)$，在不知道 $p(x)$ 的情况下，由于不能确定具体是在哪一个有限域上进行的加密运算，所以解密的难度更大。

本文还通过采用高矩阵作为密钥矩阵的方法增加了密钥空间的大小，对于一般的多项式方阵作为密钥矩阵而言，如果攻击者通过对密文长度的分析获得了密钥矩阵的阶数，则他很容易能够通过遍历这个阶的所有的多项式方阵，从而来暴力破解加密时的密钥矩阵，然而高矩阵由于行和列的数目不相同，加密后的密文长度和明文长度并不一致，因此能很好的抵御这种唯密文暴力攻击。在实际应用中可以采用更高阶的密钥矩阵，当密钥矩阵的阶越高的时候，其对应的 $k\times l$ 的多项式矩阵多达 $256^{k\times l}$ 种，而且当选取的不可约多项式 $p(x)$ 不同时，其对应的有限域也不同，从而使得暴力破解密钥矩阵更难，因此其上的 Hill 加密有更高的安全性，适合大量数据的分组加密。

6.4　平移增量

有限域 $GF(2)[x]/p(x)$ 上的 Hill 加密衍生算法 $y=\boldsymbol{A}x+\boldsymbol{b}$ 在加密时新增添了一个平移增量 $\boldsymbol{b}$，其中平移增量 $\boldsymbol{b}$ 是从加密的密钥矩阵 $\boldsymbol{A}$ 中随机选取的一列，解密的时候密文并不能直接乘以密钥矩阵 $\boldsymbol{A}$ 的伪左逆矩阵 $\boldsymbol{A}^{-1}$ 来得到明文，必须得先减去加密时候的平移增量之后做相同的操作才能解密得到明文，因为敌手不知道是否有平移增量的存在，从而加大了攻击的复杂性。

7　安全性模型

根据上节密钥的安全性及攻击复杂性分析，可以得到算法的抗攻击强度。

7.1　唯密文攻击

唯密文攻击指攻击者在仅知道已知加密文字下的穷举攻击。此时，攻击者掌握的信息最少，在本文高矩阵为密钥的 Hill 加密衍生算法中，攻击者仅根据密文并不知道对应的明文长度，不知道有限域的不可约多项式 $p(x)$，因此不能得出加密的密钥高矩阵的规模，更不知道密钥会不会是特殊的高矩阵-可逆方阵，同时也不能确定从高矩阵中随机选取的一列的平移增量。

因此算法是唯密文攻击安全的。

7.2 已知明文攻击

已知明文攻击给出了特定的明文和对应的密文，在本文的加密算法下，可以根据密文和对应明文的长度比来确定高矩阵的行数 k 和列 l 数的比例 $k:l$，尽管如此，实际高矩阵的规模则是 $tk \times tl$，因此，此时仍然不能确定高矩阵的具体规模，而且也无法确定有限域 $GF(2)[x]/p(x)$ 所选择的不可约多项式 $p(x)$。因此算法是已知明文攻击安全的。

7.3 选择明(密)文攻击

相对于唯密文攻击和已知明文攻击而言，选择明(密)文攻击是一种较强的攻击，它给与攻击者较大的权限，使得攻击者能够访问加(解)密预言机，从而得到攻击者自己构造的明(密)文加(解)密的结果，文献[17-19]提出了不同的关于 CCA 安全的公钥密码体制，选择明文攻击指攻击者获得了加密服务，选择密文攻击指攻击者获得了解密服务，在对称密码当中，这两种攻击都使得攻击者能够获得足够多的明(密)文和对应的密(明)文。此时攻击者可以通过大量的明文和密文对的信息来分析密钥矩阵的规模并进行验证。如果每次加密的密钥始终保持不变，则此时的密钥在这种攻击下是不安全的。因此，本文在上节的安全性分析当中提到可以使用一次一密来进行通信，且每次通信中每个分组使用的平移增量从密钥高矩阵的列向量中轮换选取，也即每一次通信选择的加密密钥只使用一次，使得加/解密能够保持前后向的安全性，也即保证当前密钥的泄露不会对以前的加密过程和未来的加密过程造成危害。

8 结束语

Hill 加密算法的思想对密码学的学习有很重要的意义，本文提出了一种新的有限域 $GF(2^8)$ 上的 Hill 加密衍生算法，是对经典密码学中传统的 Hill 加密算法的新的衍生，使得加密时的密钥高矩阵即使在保持固定不变的情况下，也至少能够抵抗对密钥高矩阵的已知明文攻击，因此其上的 Hill 加密相对于传统的 Hill 加密具有更高的安全性，对 Hill 密码体系的进一步深入学习有一定的借鉴意义。

参考文献：

[1] 冯克勤. 有限域 [M]. 长沙：湖南教育出版社, 1991: 24-57. (Feng Keqin. Finite fields [M]. Changsha: Hunan Education Press, 1991: 24-57.)

[2] 胡冠章. 应用近世代数 [M]. 北京：清华大学出版社, 1993: 171-193. (Hu Guangzhang, Applied recent algebra [M]. Beijing: Tsinghua University Press, 1993: 171-193.)

[3] 万福永，戴浩晖. Hill_2 密码体系加密过程中的哑元问题 [J]. 数学的实践与认识, 2007 (8): 87-90. (Wan Fuyong, Dai Haohui. The design of dummy variable in hill2 coding system [J]. Mathematics in Practice and Theory, 2007 (8): 87-90.)

[4] 杨淑菊. Hill 密码的加密解密矩阵的求法 [J]. 价值工程, 2016 (26): 285-287. (Yang Shuju. Method for encryption and decryption matrix of hill cipher [J]. Value Engineering, 2016 (26): 285-287.)

[5] 徐小华，黎民英. Hill 密码加密解密时矩阵的求法 [J]. 电脑与信息技术, 2010 (2): 31-33. (Xu Xiaohua, Li Minying. The solution of matrix of hill cipher in encryption and decryption [J]. Computer and Information Technology, 2010 (2): 31-33.)

[6] 王容，廖群英，王云莹，曾茂俊，宁宇光，洪思奥. Hill 加密算法的改进 [J]. 四川师范大学学报：自然科学版, 2015 (1): 8-14. (Wang Rong, Liao Qunying, Wang Yunying, *et al*. Improvement of hill encryption algorithm [J]. Journal of Sichuan Normal University: Natural Science, 2015 (1): 8-14.)

[7] 付卫平，陈继业. 有限域 GF (2~n) 的一种除法运算算法 [J]. 邵阳学院学报：自然科学版, 2015 (2): 3-10. (Fu Weiping, Chen Jiye. An algorithm to implement division operation of finite field GF (2~n) [J]. Journal of Shaoyang University: Natural Science Edition, 2015 (2): 3-10.)

[8] 蒲保兴，王伟平. 线性网络编码运算代价的估算与分析 [J]. 通信学报, 2011 (5): 47-55. (Pu Baoxing, Wang Weiping. Evaluation and analysis of the computation cost of linear network coding [J]. Journal on Communications, 2011 (5): 47-55.)

[9] 焦占亚，曾永莹，刘海峰. 一次一密的密码算法研究 [J]. 西安科技大学学报, 2005 (4): 477-480. (Jiao Zhanya, Zeng Yongying, Liu Haifeng. Design and realizing of a system of block cipher [J]. Journal of Xi’an University of Science and Technology, 2005 (4): 477-480.)

[10] 谢邦杰. 线性代数（第一版）[M]. 北京：高等教育出版社, 1978. (Xie Bangjie. Linear algebra (first edition) [M]. Beijing: Higher Education Press, 1978.)

[11] 王松桂. 广义逆矩阵及其应用 [M]. 北京：北京工业大学出版社, 2006. (Wang Songgui. Generalized inverses and applications [M]. Beijing: Beijing University of Technology Press, 2006.)

[12] 张玉安，冯登国. 一种实用的仿一次一密分组加密方案 [J]. 北京邮电大学学报, 2005 (2): 101-104. (Zhang Yu’an, Feng Dengguo. A practical one-time-pad-like block cipher scheme [J]. Journal of Beijing University of Posts and Telecommunications, 2005 (2): 101-104.)

[13] 刘海峰，吴鹏，马令坤. 基于有限域上圆锥曲线的分组加密算法及实现 [J]. 吉林大学学报：理学版, 2012, 50 (1): 54-58. (Liu Haifeng, Wu Peng, Ma Lingkun. Implementation of group encryption algorithm based on conic curve over finite fields [J]. Journal of Jilin University: Science Edition, 2012, 50 (1): 54-58.)

[14] 卢开澄. 计算机密码学——计算机网络中的数据保密与安全（第 3 版）[M]. 北京：清华大学出版社, 2003. (Lu Kaicheng. Computer cryptology-data privacy and security in computer networks (third edition) . [M]. Beijing: Tsinghua University Press, 2003.)

[15] 刘海峰，何立勇，郭改慧，等. Hill 密码体系中的加密矩阵与哑元 [J]. 西南大学学报：自然科学版, 2014 (11): 138-142. (Liu Haifeng, He Liyong, Guo Gaihui, *et al*. The dummy and encryption matrix in the Hill coding system [J]. Journal of Southwest University: Natural Science Edition, 2014, 36 (11): 138-142.

[16] 卿斯汉. 密码学与计算机网络安全 [M]. 北京：清华大学出版社，2001. (Qin sihan. Cryptography and computer network security. [M]. Beijing: Tsinghua University Press, 2001.)

[17] 李素娟，张明武，张福泰. 抗 (持续) 辅助输入 CCA 安全的 PKE 构造方案的分析及改进 [J]. 计算机学报，2017: 1-13. (Li Sujuan, Zhang Mingwu, Zhang Futai. Security analysis and improvement of CCA secure PKE with (continual) auxiliary input [J]. Chinese Journal of Computers, 2017: 1-13.)

[18] 王欣，薛锐. 对于一个新的 CCA 安全的密码方案的分析 [J]. 密码学报，2017 (2): 106-113. (Wang Xin, Xue Rui. Analysis of a new CCA-secure public-key cryptosystem [J]. Journal of Cryptologic Research, 2017 (2): 106-113.)

[19] 王占君，马海英，王金华. 基于适应性选择密文不可区分性的抗辅助输入泄漏公钥加密方案 [J]. 计算机应用，2014 (5): 1288-1291. (Wang Zhanjun, Ma Haiying, Wang Jinhua. Public key encryption scheme with auxiliary inputs based on indistinguishability under adaptive chosen ciphertext attack [J]. Journal of Computer Applications, 2014 (5): 1288-1291.)